

volume 1, issue 1

www.microsoft.com/protect

safety and security online

Microsoft®

protect your computer, yourself and your family

inside

online safety
and security
is all about you





Kristin Johnsen
Senior director
of security outreach
Security Technology Unit
Microsoft Corp.

letter of introduction

Can you remember the first time you ventured onto the Internet? I can. I remember feeling like my world had suddenly multiplied in size. I have been involved with computers for a long time, starting as a programmer over 15 years ago. However, it was in about 1996 that the Internet began to change my life. It was in that year, when I was working as a consultant traveling the globe, that all of a sudden e-mail became a substitute for voice mail, and business information was available online rather than only through research teams. Collaboration on projects across the globe became possible since we had the opportunity to communicate. Needless to say, a world of new opportunities opened up, increasing my reach and my connection with others, and enabling me to use real-time information in decision-making.

Today the Internet is no longer new or novel to most of us. A 2005 study by the Pew Internet & American Life Project found that more than two-thirds of Americans are now using the Internet. They use it to communicate with friends and family, pay bills, comparison-shop in a worldwide marketplace, watch movies, and perform other tasks that would have seemed impossible even a decade ago. However, high-profile cases of online identity theft, child exploitation and computer viruses are quite understandably fueling concern about safety and security on the Web. The economic impact of these online threats is steadily rising as well; because of viruses and spyware, over the past two years American consumers spent at least \$7.8 billion for computer repairs, parts and replacement, according to the 2006 Consumer Reports “State of the Net” survey.

All of us who enjoy and benefit from the Internet also play a vital role in helping make and keep this valuable resource safe and secure. To help ensure a more trustworthy Web experience, parents and their kids first need to clearly understand the risks that exist online. The good news is that today’s online threats are for the most part manageable and avoidable, and there are solutions — both technological and behavioral — for the various problems and risks. Microsoft Corp. and its partners have developed this publication, **Safety & Security Online**, to share a broad range of security information, tools and other resources available to help people protect their PCs, themselves and their families online.

As you read on, you will find easy-to-understand online security guidance tailored to the interests and concerns of specific groups: parents, teens, kids, and seniors. Through this and many other educational resources within Microsoft’s ongoing Trustworthy Computing efforts, we aim to put people in control of their information and give them the opportunity to realize the full potential of the Internet. We are doing this through the following means:

- Making our products more secure out of the box, including our flagship operating system, Windows.
- Providing a broad range of additional security-enhancing tools for consumers.
- Bringing helpful information to the public by collaborating with other companies and advocacy groups to organize activities, such as through the creation and maintenance of <http://www.staysafe.org>, an independent Web site that provides an array of Internet safety resources.
- Helping law enforcement and government agencies crack down on online criminals through joint educational efforts and new technology.

You will see evidence of these and other efforts throughout **Safety & Security Online**. We hope these resources will inspire you to take a closer look at your own online safety habits as well as those of your family. Microsoft and its industry partners would like you to spend your online time realizing your personal potential, using the Internet safely to help reach your goals.

Be safe and secure online,
Kristin

safety and security online

2 Letter of Introduction

Kristin Johnsen, Microsoft senior director of security outreach, discusses online safety and what Microsoft is doing to help people protect their PCs, themselves and their families online.

4 New Safeguards, Education and Law Enforcement Ease Web’s Growing Pains

Featuring commentary from a real victim of cybercrime, this feature story describes the threat of cybercriminals and tells how law enforcement is taking action against online crime. Learn how to be cybersmart in your online ventures.

8 Technology Solutions

A sampling of security products and services, and advice on choosing the best options for your security needs.

11 Bridging the New Generation Gap: Straight Talk and Advice on How Parents Can Help Protect Their Kids Online

Real-life accounts of the importance of online safety, from the perspective of consumers and their families expressing real-life concerns about safety and security on the Internet.

17 Acronyms 101: Understanding Online Jargon

A quiz for households with children online. Do you know what your children are really talking about online?

18 Online Safety Advocates Boost Efforts to Educate Older Consumers

A real-life account of cybercrime from the perspective of a cybervictim. Read her story to learn what she did to get even and how you can help protect yourself from similar crimes.

21 Don’t Get Trapped in Your Own Web Social Circle

Tips and tricks for those who blog and use social networking sites. Learn more about safe ways to share your information online.

24 Working Together to Increase Online Safety and Security

When organizations work together, they can communicate strong messages to a wide-reaching audience. This feature outlines Microsoft’s work with several organizations to help educate consumers on the best practices for online safety.

27 Online Safety Information Cards

For quick reference, these information cards provide quick online safety guidance, tips and resources. Easy to cut out so you can keep them handy

cover story

parents

50+

teens

partnership

new safeguards, education and law enforcement ease the web's growing pains

After hurricanes Katrina and Rita, the Internet demonstrated its power. And, as reliance on the Internet hit new highs, online criminal activity soared to new heights as well.

Almost overnight, scam artists went on a "phishing" spree, soliciting donations online to phony charities via e-mails that directed people to equally phony Web sites designed to look like those of trusted companies. Business was so brisk that Katrina-related Web domain names were being sold through online auction sites, with starting bids as high as \$15,000, according to The Washington Post in August of 2005.

Welcome to the Internet's difficult adolescence. As the Web has matured from fad to work tool and now to a daily necessity for tens of millions of Americans, the potential risks unleashed by hackers and criminals have also matured. A seemingly constant stream of media reports tell of Web-borne threats: computer viruses that can damage millions of computers in one fell swoop, spyware and phishing attacks that fuel nationwide identity theft, and personal networking services that can be misused to lure children and other unsuspecting Internet users.

Much of the hope for increased Internet safety rests with a new generation of easy-to-use and comprehensive Internet security products, as well as a fundamental change in the way technology is developed: with security in mind from the ground up. This maturation also hinges on people taking advantage of these products and educating themselves through the broad variety of guidance available from online companies, law enforcement officials and consumer advocacy organizations.

And, despite studies that indicate a majority of consumers are still vulnerable to online criminal activity, Kristin Johnsen, senior director of security outreach for Microsoft's Security Technology Unit, is optimistic. "If people know about the online risks, follow the right safety steps and use technology to help protect themselves, they can almost always be avoided," Johnsen said.

16 million instances of malicious software from 5.7 million computers by running a monthly scan for malicious software during the 15 months after its January 2005 debut.

- Windows XP Service Pack 2 has reduced the number of critical vulnerabilities compared with the previous version of Windows XP, according to internal Microsoft analysis.

vocabulary lesson

PHISHING PRONOUNCED\FISH-ING\

v. A method of identity theft carried out through the creation of a Web site that seems to represent a legitimate company **USAGE** Online criminals pretend to be legitimate businesses to phish for personal information.

- Windows Live OneCare, an all-in-one, automated PC Care service that combines anti-virus, anti-spyware, firewall, data-backup and restore protection features, as well as tune-up features and around-the-clock online support.

Covering All the Security Bases

Consumer Joe Macher is among the latest converts to this new generation of security software. Macher's two home PCs began to slow and crash earlier this year after he downloaded some free online games for his grandkids. The retired paper-industry supply engineer thought his old security software would protect his PCs if any spyware was stowed away in the games; it didn't. "The games looked fun and innocent enough," he said. "But in the background, someone was busy loading up my machine with spyware, adware and viruses."

When both computers began slowing and crashing, Macher realized that he had to do something and do it quickly. He looked to newer security programs; in the end, the Windows Defender beta — a free download from Microsoft — uncovered the spyware that was causing the problems,

and Macher was able to eliminate it by having a technical support person help him reload his operating system.

Macher is one of the millions of people who have downloaded the Windows Defender beta since its debut. In addition to Windows Defender, Microsoft offers a variety of security offerings to help protect the computing experience:

- Stand-alone security software products including the Malicious Software Removal Tool (MSRT), which removed

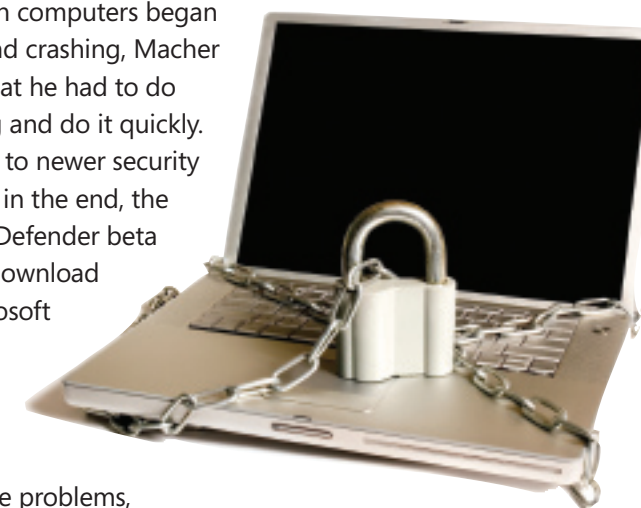
- In addition to its fully managed "take care of everything for me" service, Windows Live OneCare offers consumers certain free services such as Windows Live OneCare Family Safety, OneCare Advisor and Windows Live OneCare Safety Scanner. Windows Live OneCare Family Safety is a free safety service in beta form that will include content filtering for the Web, contact list management tools for communication services, and online activity reports. OneCare Advisor is also available free as a part of Live Toolbar; it provides quick and easy access to the Windows Live OneCare Safety Scanner, a free, on-demand online resource to help consumers protect themselves and keep their PCs running well, as well as an updated version of Microsoft Phishing Filter that includes additional functionality to help protect consumers from online data theft.

- SmartScreen® Technology, which helps fight spam and phishing, is available across e-mail platforms from Microsoft to help protect users from unwanted e-mail.

- The Microsoft Phishing Filter is also available in the Live Toolbar and Windows Internet Explorer® 7 to help protect customers from rapidly evolving phishing scams.

"Software services, such as Microsoft Automatic Updates, are also helping increase online security," said Microsoft's Johnsen. These services can automatically download software updates to your computer that help protect against new threats, like viruses or worms and other potential computing security vulnerabilities before they become issues.

"This helps keep your Windows-based computer protected and up to date against potential threats," Johnsen said. "It also gives consumers a good feeling that their machine is safer."



7.8 HOURS
PER WEEKCOMMUNICATING WITH FRIENDS
VIA COMPUTERS OR CELL PHONES10.3 HOURS
PER WEEKDOING SOCIAL ACTIVITIES
OUTSIDE OF SCHOOL

Source: Paul Hitlin, Amanda Lenhart, Mary Madden, "Teens & Technology: Youth Are Leading the Transition to a Fully Wired and Mobile Nation," Pew Internet & American Life Project, July 27, 2005. http://www.pewinternet.org/PPF/r/162/report_display.asp

Getting Cybersmart

Equally encouraging, Johnsen said, is the mainstream media's increased attention to Internet security. "There are daily news reports about the dangers posed by worms, viruses and online predators," she said. "Consumers are getting the message that there is a need to be careful so their family can get and stay cybersafe."

The good news is that people don't have to look far to find abundant resources, most of which are available at no charge. People can take their choice of trusted advocacy groups and organizations, from technology companies such as Microsoft (<http://www.Microsoft.com/protect>) to sites that combine the knowledge and perspectives of numerous organizations, such as GetNetWise (<http://www.getnetwise.org>). In addition, community-based sites such as <http://www.staysafe.org> compile guidance from several different sources: i-SAFE, Microsoft, NCMEC, NetFamily News, Net-Mom Approved, OnGuard Online and SafeKids.com.

Many of the organizations dedicated to online safety are banding together to take their safety and security lessons on the road, through nationwide or regional tours. The Get Net Safe Tour, traveling to 12 cities across the United States, is a joint effort by Microsoft and 10 other organizations to offer safety education events for students, parents, teachers, those over age 50, and government and community leaders across the country.

Macher believes that taking the time to learn about how to stay safe online is as important as implementing a security technology.

"You really need to educate yourself," Macher said. "Attend an informational seminar; sit down with a cybersavvy friend, or visit one of the Web sites. Just make sure you learn the do's and don'ts before you do something silly like I did."

Cracking Down on Cybercriminals

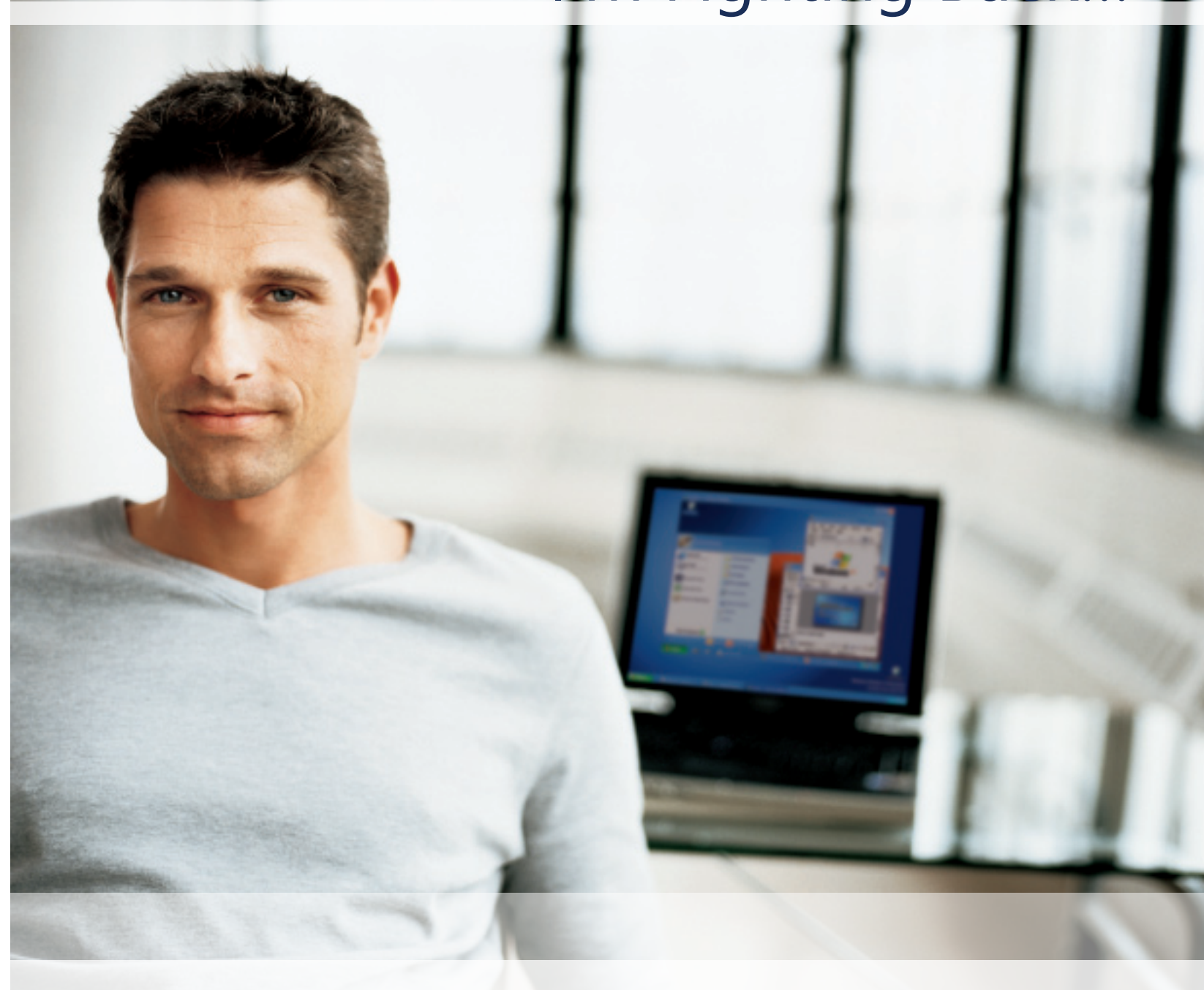
Macher and other Internet users benefit from another type of security effort, even though they aren't the target audience: Law enforcement agencies are taking action against cybercriminals, which in turn helps all Internet users. Joint efforts — which often combine the resources of Microsoft, law enforcement and other organizations — have led to hundreds of cases legal action against spammers, phishers and other cybercriminals worldwide. Most notably Microsoft and the New York state attorney general sued spammer Scott Richter (formerly known as the "Spam King"), resulting in a \$7 million settlement in August 2005 for Microsoft. Efforts like this send the message to others thinking of sending spam that it's a crime. Microsoft then donated the settlement funds to further technology and education efforts.

By closely tracking malicious code and rapidly alerting law enforcement when outbreaks occur online, technology companies are reducing the spread of worms and other destructive software and are helping to bring cybercriminals to justice. Microsoft is in a unique position to help law enforcement combat cybercrime, because it can document the activity and provide the evidence needed to bring a case to court. Providing law enforcement with resources, expertise and information that make it easier for them to prosecute cybercriminals is not only the right thing to do, it helps keep the Internet safe.

Pre-emptive efforts have produced new law enforcement tools such as CETS. Developed by Microsoft, the Royal Canadian Mounted Police (RCMP) and the Toronto Police Service, CETS software tools and technologies help make it possible for law enforcement to capture, share and search for information worldwide about online child-exploitation cases. Several countries have expressed an interest in the system since the tool was unveiled in Canada in 2005. Most recently, Indonesia adopted CETS in June 2006, and Microsoft is working with governments and law enforcement agencies worldwide on future CETS rollouts.

As the Internet outgrows its adolescence, lessons learned through Hurricane Katrina's massive online response and experiences like Macher's spyware attack show that some level of crime on the Internet will likely always exist. However, if people's awareness about how to help protect themselves online matures along with the Internet, many online threats may be avoided and people can positively experience all the Web has to offer.

I'm Fighting Back...



Microsoft has provided special training to more than 15,000 of its developers, program managers and testers on how to build more secure computer code — and this training is regularly updated to help these

employees keep up with changes in security threats. More secure code makes it harder for hackers and thieves to break into your home PC, and is just one of the enhanced processes in Microsoft's Security Development Lifecycle.



technology solutions

helping people better protect their PCs, themselves and their families for a safer computing experience

Many people experience frustration when they try to protect their PCs, themselves and their families online. Although some understand the importance of staying safe while on the Internet, with all the options available it is often hard to know what you and your family should use. Here are some security products and services, and some related advice on choosing the best options for your computer security needs.

Firewall

A must-have security feature for those who don't yet have Windows XP Service Pack 2, Windows Live OneCare or another security offering with a built-in firewall.

For more information and download details, visit <http://www.microsoft.com/protect>.

Software updates

Online services, such as Microsoft Automatic Updates, help ensure that your PC has the most current updates and protections for today's ever-evolving online threats. These updates can be delivered and loaded onto your PC via the Internet automatically — with your permission, of course.

For more information and for installation instructions, visit <http://update.microsoft.com>

Windows XP Service Pack 2 (SP2)

This update to the Windows XP operating system is all about security improvements, and it's one of the most important service packs ever released. For those who already have Windows XP, this all-in-one update includes the following:

- Windows Firewall helps defend your computer against viruses and intruders trying to access your computer over the Internet.
- Windows Security Center is a command central for managing your Windows XP security settings, including firewall status, automatic update settings and virus protection.
- Pop-up Blocker gives you more control of your Internet browser by stopping most pop-up ads.

For more information and download details, visit <http://www.microsoft.com/windowsxp/default.mspx>.

Anti-virus software

Don't let a computer virus or other unwanted software ruin your online experience. If you don't use OneCare, make sure you seek out other anti-virus software — and follow the recommendations for keeping it up to date.

For more information and download details, visit <http://www.microsoft.com/protect>.

Anti-spyware software

To provide optimal anti-spyware protection, Microsoft developed Microsoft Windows Defender:

- Windows Defender. In addition to helping defend against pop-up ads, slow performance and security threats caused by spyware and other unwanted software, this service offers a user interface that adapts how it alerts you based on the severity of a threat. This reduces intrusion while helping ensure urgent threats don't go unnoticed.

Available at <http://www.microsoft.com/windowsdefender>.

additional microsoft safety and security solutions

Windows Live OneCare

This is a favorite with those who don't have a lot of time or want to help ensure that their security software works well together. Windows Live OneCare is an all-in-one PC care service that manages protection, maintenance and backup, so customers don't have to worry about protecting and maintaining their PCs. It performs the following protective duties and PC maintenance:

- Anti-virus protection features remove viruses, worms and Trojan horses, based on a continually updated list of threats.
- Windows Defender defends against pop-up ads, slow performance and security threats caused by spyware and other unwanted software.
- Two-way firewall checks for threats in incoming data — as well as viruses or stealth programs, such as zombies or spyware — that can run unnoticed in the background and send information from your computer to the Internet.
- Performance tune-ups automate tedious but important maintenance tasks, such as cleaning up your hard disk and reassembling broken files and other faults that can slow PC performance. They also install updates to Microsoft operating systems.
- Backup a restore service helps re-create lost files — including those you may accidentally delete — and create an extra copy of valuable files on CD, DVD or an external hard drive. The service also puts things back where you left them; you don't even have to remember where they

were on your PC to get them backed up or restored.

- Online support provides e-mail, phone and chat support with any subscription for no additional charge. An around-the-clock automated online service lets you type your questions in plain language (for example, "How do I block a program in the firewall?"). Responses include a series of steps to perform a task or links to more instructions.

Available at <http://onecare.live.com>.

Malicious Software Removal Tool

Checks computers with Windows XP, Windows 2000 and Windows Server® 2003 for specific, prevalent malicious infections and helps remove any infection found. Microsoft releases an updated version of this tool once a month and as needed to respond to security incidents.

Available at <http://www.microsoft.com/security/malwareremove>.

Microsoft Phishing Filter

Provides immediate alerts if you visit a Web site that displays characteristics of or is a known phishing site. If you are using the Internet Explorer 7 beta or the Windows Live Toolbar, you can opt in to use the Phishing Filter.

Available at <http://toolbar.live.com> or <http://www.microsoft.com/windows/ie/default.mspx>.

Windows Live OneCare Safety Scanner

Scans and checks your PC's health, and helps delete viruses and other threats. It also provides you with access to an online support community where you can learn about the latest security issues.

Available at <http://www.safety.live.com>

Windows Live Toolbar

In addition to linking to Windows Live Search, offers OneCare Advisor, enabling easy access to the Windows Live OneCare Safety Scanner and an enhanced version of the Microsoft Phishing Filter.

Available at <http://toolbar.live.com/features.aspx>.

Family Safety Technologies

Helps parents manage what their children do and who they communicate with on the Web. Available online through Windows Live OneCare Family Safety and in the Windows Vista operating system through Parental Controls, these settings offer choices based on whether the technology is loaded onto your computer directly in the operating system or is a part of the beta Windows Live experience.

Windows Live OneCare Family Safety is a Web-based service that applies to online content and services and will include contact management features that will enable parents to create "allow" lists for other Windows Live beta services, such as Windows Live Messenger and Windows Live Spaces, in the coming months. Its settings are active when a customer signs in to the beta version of Windows Live on PCs that have Family Safety software installed, and parents can monitor online activity reports and update settings from virtually any PC. Similarly, the Family Safety Parental Controls feature offered in Windows Vista is a PC-based service that will provide security and safety measures to the computer on which Windows Vista is installed, and also extends a level of control in offline areas too, such as for PC games.

Also, for the gamers there are easy-to-use Family Settings in the Xbox 360™ system and Xbox Live®, with the goal of protecting children from both inappropriate content and contacts. The features create several opportunities for parents to decide the level of their children's access in Xbox Live, and also limit the possibility for children to create Xbox Live accounts without the knowledge of their parents.

Windows Live OneCare Family Safety is available at <http://www.ideas.live.com>. Prices for Xbox 360 systems and Xbox Live subscriptions vary.

bridging the new generation gap straight talk and advice on how parents can help protect their kids online

The generation gap that separates parents from their kids has been around for, well, generations. But bridging this divide is getting more challenging than ever for parents. In addition to music, fashion and politics, moms and dads are now struggling to relate to, teach and guide their kids when it comes to computing activities.

While most parents use the Internet at work or to pay bills, their kids and teens use it to explore, learn and communicate with their friends in ways that previous generations couldn't have imagined. The Internet is a seamless digital playground for them to create their identities in

social networks, create personal Web pages and online journals called "blogs" (short for Web logs), and download music and play games. For example, according to a 2006 Burst Media survey, more than 80 percent of all U.S. teens are online at least one hour a day, roughly three out of five have visited a social networking site, and of those teens about 60 percent joined a social networking site and created a profile. These activities have many benefits, but they also raise personal safety and security issues if parents haven't educated themselves, guided their children and set up adequate Internet safeguards for their children.

Safety & Security Online

met up with several moms and dads to find out what they are doing to help keep their children safe online. The conversation and questions centered on how they speak with their kids about the benefits and risks on the Internet, how they monitor and regulate their children's Internet use, and what are some tips for parents seeking online safety advice. Participating in the discussion were the following:

- **Triva**, an administrative assistant who is married to Toby. They have two children: Courtney, 12, and Taylor, 10.
- **Diane**, a payroll professional who is married to Alan. They have two children: a daughter, 9, and a son, 5.
- **Dan**, a teacher who is married to Kass. They have a son: Max, 15.
- **Jessica**, a retail salesperson and single mother. She has a son: Blake, 11.
- **Kristin Johnsen**, senior director of security outreach in the Security Technology Unit at Microsoft Corp. She and her husband, Duane, have two children: Jared, 6 and Noah, 9.
- **Dr. Donald Shifrin**, chair of the American Academy of Pediatrics (AAP) Committee on Communications. He is married to Bobbi; they have two children: Max, 15, and Alexis, 12.

Q: An i-SAFE survey found that almost a third of children in grades 5–12 have visited an inappropriate Web site. Another survey by i-SAFE found that more than half of kids trust people with whom they chat online, even if they have never met them in person. Do these kinds of statistics scare you?

Jessica: Sure. I know my son is too trusting of what he sees online. It took me a few times to explain to him that the pop-ups don't really mean you've won.

Johnsen: Parents need to know that they can do a great deal to protect their kids online. And the good part is, they don't have to be technology experts. The same common-sense rules we teach our children to protect themselves in the physical world — such as not accepting gifts from strangers — also apply to keeping them safe in the virtual world. We need to understand the risks, have clear guidance for healthy online behavior, use technology where it can help, and talk openly with our kids.

Q: How often do you speak with your kids about the risks on the Internet?

Triva: We discuss everything that could happen. We don't try to scare them, but we want them to be aware of the realities and want them to be able to share their experiences with their parents.

Jessica: We talk about once a week. I'm really open and really specific with the guidance I give my son. My greatest fear is that someone with a fake profile will attempt to befriend him online. But I've told him over and over to treat people he meets on the computer like he would any stranger: If you don't know them, don't chat with them, and if you're concerned about your online communications, click off and tell your parents.

Dr. Shifrin: Surfing the Web should be like driving a car. We don't just wait until our children turn 16, give them a driver's license, put them in a car and send them off. We educate them and drive with them until we trust that they are driving safely. Similarly, with the Internet, we encourage parents to get involved sooner rather than later, since they will be on the Internet, and we want them to surf safely.



Q: How do you regulate how and when your kids use the home computer or other gaming systems?

Johnsen: I have set up a separate account for them on our family computer. All you have to do is go into the control panel within Windows XP, then look for User Accounts. Inside there you can set up what's called a "limited-user account." This helps prevent them from adding software or downloading malware off of the Internet, or changing most computer settings or their personal account permissions. There are step-by-step instructions on how to do this at <http://www.microsoft.com/protect>.

Jessica: I let my son use the computer for an hour each night after I get home from work. It's hard to enforce. He tries to get onto IM whenever he thinks I'm not watching. I try to keep track of who he IMs with by checking his buddy list. I also keep telling him never to give out information like our address or his name.

Q: How can parents like Jessica enforce their rules? She can't constantly hover around the PC, can she?

Johnsen: Of course not. That's why parents need to also install individualized safety settings for each child that help them establish guidelines for online activity, such as on the new Windows Live OneCare Family Safety, which is currently in beta; the new settings that will be in Windows Vista; or the settings in MSN® Premium and the Xbox® gaming system. These filters help block kids from inappropriate stuff, such as adult Web sites or violent games. My husband and I are usually watching over our kids' shoulders when they are online, but when we aren't the guidelines that we've set up help stop our kids from going places and contacting people we don't want them to online.

Dr. Shifrin: The Windows Live OneCare Family Safety beta is designed to give parents lots of flexibility to help create an environment of trust between parents and children. Family Safety is designed to promote this kind of trust, giving parents more confidence in knowing what their children are doing while allowing kids to more safely explore and enjoy the Internet. It also is designed to engage parents and kids in conversations about the Internet. For example, if the report shows that a 16-year-old is spending a lot of time on a certain commercial site, the parent can discuss with the child why that is and determine how to proceed.

where to start

Here's a handy list of online resources that can help parents get up to speed with online security.

Microsoft Protect. This web site will provide you with the tools and information to help protect your PC, your information and your family. <http://microsoft.com/protect>.

i-PARENT. This is a nationwide movement of students, parents, educators and public officials to inform parents about the dangers kids face online and offer tips to help protect them: <http://www.ilearn.isafe.org>.

StaySafe.org. This is an all-inclusive Web site, developed by Microsoft and other online security advocates, that offers information and resources geared to different age groups and interests: <http://www.staysafe.org>.

Xbox Family Settings. This site explains how parents or system owners can set permissions that allow all members of the household to enjoy Xbox in a user-appropriate environment: <http://www.xbox.com/familysettings>.

Q: Where is your family's computer located in your house?

Johnsen: We've got it where online safety experts say it should be: in a common room, so we can monitor what they are doing — or at least make them think we are.

Jessica: I agree. As children get older and more savvy online, the PC should be in a place where you can easily monitor what they're up to. Right now, we have the family computer in the home office, which the children have limited access to. Our daughter has an older PC in her room. It's loaded with educational or artistic games and programs for the kids, and isn't connected to the Internet.

Triva: Our computer is in the room that my husband and I use as our bedroom and family office. We plan to move it into our upstairs sitting room when the kids are older.

vocabulary lesson

MALWARE
PRONOUNCED \MAL-WARE\

n. Software, such as viruses, intended to damage or disable a computer system; short for malicious software
USAGE Setting up security for your PC is the best way to guard yourself against malware.

e-mail and on a social networking site. We talked to her about what is appropriate and what isn't, as well as the risks of sharing too much personal information online. Her parents aren't very computer-savvy, so we explained to them what was going on. Now they're communicating more about their online activities.

Q: Who do you feel is responsible for protecting your family online?

Diane: I feel it is a shared responsibility between the online providers, the software industry, and you as the individual choosing to go online. First of all, you as a family need to be careful about how much personal information you share online, if at all, and what you access online. The

technology and software industry should provide more spam- and hacker-blocking tools along with you choosing services that help protect your PC and family. It's kind of like anything in life: You have to be responsible enough to make smart choices in purchasing, accessing and using the product. If you abuse it, you are making the choice to potentially get burned.

Jessica: I suppose it should be me, but I don't know where to start. I have a hard time doing personal research. I'm a

Q: How do you feel about social networking sites?

Triva: We don't let our kids visit social networking sites, chat rooms or online auctions; they're still too young.

Johnsen: Our kids aren't yet interested in social networking. But when one of our teenage relatives came to stay with us over Christmas, we discovered that she was involved in some less-than-appropriate conversations on



in my children's Parent Teachers Association, so I've recommended we put on a Parent Night about computer security and child safety. This is something any concerned parent can do to learn more themselves and help spread the word about online security.

Q: Would you ever review your kids' e-mail?

Dan: It would depend on the situation. I am very trusting of my son's ability to make appropriate decisions. As he proves he can handle responsibility, we give him more.

Jessica: Yes, I would check my son's mail. At times, I wish I had a log of what was discussed on his instant messages as well.

Johnsen: You can. Windows Live OneCare Family Safety will offer reporting options on where your

children are going on the internet and who your children communicate with. This isn't a mechanism for spying on your kids — they know in the setup of the service that you're monitoring them — but more of a tool for any discussions you need to have with them. It also puts some control in the hands of parents, having tools to discuss with them how they manage who they communicate with online.

Johnsen: You're not alone. Before I began working in online security, I did not know about all the safety issues and security risks online. But you really don't have to do much research online these days to find a ton of great resources. One of the best places to start is Microsoft.com. Just type in "Protect children online" in the Search bar. Or, visit Stay-Safe.org. It's a site, created by Microsoft and a number of other trusted organizations, that's like a clearinghouse of information and links to other online safety resources.

Q: What else can parents do to learn about online security?

Johnsen: If you prefer more interactive advice, try the Security for Home Users Newsgroup on Microsoft.com. It's an online spot monitored by technology professionals and enthusiasts, who answer online security questions and provide free, expert advice. People can post questions, review other postings or offer their own advice.

Or, you can do what I've done: My husband is very active

children are going on the internet and who your children communicate with. This isn't a mechanism for spying on your kids — they know in the setup of the service that you're monitoring them — but more of a tool for any discussions you need to have with them. It also puts some control in the hands of parents, having tools to discuss with them how they manage who they communicate with online.

Q: Do you have any other tips for parents who are seeking online safety advice?

Johnsen: I mentioned this earlier, but it's super important: Encourage your kids to be open with you. This way, if they see something on the Internet that makes them feel uncomfortable, they have someone to talk to about it without fear of getting their computer privileges taken away.

Triva: Don't be afraid of the tough questions; just answer them honestly. If kids receive straight answers, they tend to make better choices.

Dan: Remove their fingers (laughing). Just kidding.

a parent's guide to online safety

ages and stages



ideas for 12+ year olds



- Teach your teen not to download programs, music or files without your permission. File sharing and taking text, images or artwork from the Web may infringe on copyright laws and can be illegal.
- Help protect them from spam.
- Make sure your teen checks with you before making financial transactions online, including ordering, buying or selling items.
- Discuss online gambling and its potential risks.

ideas for 9 to 12 year olds

- Insist that your kids agree never to meet an online friend.
- Allow your kids to use only monitored chat rooms on reputable kids' sites.
- Talk to your kids about online pornography and direct them to good sites about health and sexuality.
- Insist on access to your kids' e-mail and instant messaging accounts to make sure they're not talking to strangers.
- Talk to your kids about responsible, ethical, online behavior to avoid gossiping or bullying.



ideas for 7 to 8 year olds

- Establish a shared family e-mail account with your Internet service provider rather than letting your kids have their own accounts.
- Teach your kids not to download software, music or files without your permission.
- Talk to your kids about their online friends and activities.
- Make sure your kids do not download software, music or files without your permission.

ideas for 5 to 6 year olds



- Supervise your kids' activities by keeping all Internet-connected computers in open areas
- Tell kids never to give out information about themselves or their family
- Don't let your kids use instant messaging, e-mail, chat rooms or message boards.
- Encourage your children to tell you if something or someone online makes them feel uncomfortable or threatened.

ideas for 2 to 4 year olds

- Always sit with your kids.
- Add acceptable sites to your Favorites List.
- Use kid-friendly search engines. (such as MSN Kids Search).
- Investigate Internet-filtering tools.
- Use pop-up window blockers.
- Help your kid create an online nickname to ensure privacy.



acronyms 101

figuring out online jargon

Think how hard it would be to monitor your children's telephone conversations if they spoke another language. Well, many teens use a different language online — one that includes dozens of acronyms for frequently used phrases. This language allows teens to more quickly communicate in the rapid-fire online world of instant and text messaging. But it can also help them disguise activities from their parents, and enable predators to illicitly communicate with kids.

If you want to know what your kids are talking about via e-mail, instant messaging or text messaging, you need to be able to speak the language and use the acronyms like they do. In the following list of eight commonly used acronyms; see how many you know. Check your answers below:

- | | |
|---------|----------|
| 1) POS | 5) LMIRL |
| 2) ASL | 6) KPC |
| 3) WYRN | 7) WYCM |
| 4) IBN | 8) OLL |

To learn more online jargon, visit these Web sites:

http://www.staysafe.org/parents/iresources/chat_acronyms.html

<http://www.microsoft.com/protect>

- Answers:
1. Parents over shoulder. Other related acronyms: PIR (Parents in room); P911 (Parent alert); PAW (Parents are watching)
 2. Age, sex, location
 3. What's your real name?
 4. I'm buck naked
 5. Let's meet in real life
 6. Keeping parents clueless
 7. Will you call me?
 8. Online Love



Microsoft has built a worldwide security response system to protect you and other customers from online threats and vulnerabilities. The Microsoft Security Response Center scours the Web for word of potential online threats and maintains a email address, secure@microsoft.com, for security incident reports, which we monitor 7 days a week, 365 days a year. When security incidents occur, the MSRC responds quickly and aggressively with information and fixes. The MSRC's got your back online.



GROWTH CHART



online safety advocates boost efforts to educate older consumers

Washington state resident joins AARP and Microsoft campaign to fight back against cybercriminals.

Judy Melloon's heart sank as she reviewed her monthly bank statement. The account should have contained several hundred dollars. It was empty.

A long list of ATM withdrawals had been made overseas, although it had been weeks since she or her husband used their ATM card or ventured any farther than the local grocery store. In fact, the only time she had thought about the account all month was when she received an e-mail request from a trusted company to update her account information. It was the latest of several requests, so she clicked on the Web link in the e-mail and typed in the requested information. A few hours later, the overseas withdrawals began.

Melloon is not alone. Internet-related fraud complaints from people over 50 years old are increasing. In fact, the Federal Trade Commission found that Internet-related complaints in 2005 accounted for 37 percent of all reported fraud complaints from consumers age 50 and over, with monetary losses of more than \$72 million and a median loss of \$300. Melloon simply responded to an e-mail request to update her billing information with a company that she regularly does business with online. However, the message was not sent by the company, but by an online scam artist who mimicked the design of the company's Web site and logo to make the correspondence appear legitimate.

But Melloon refused to be just another crime victim tricked by a scam artist. Instead, she began educating herself about online safety and security, so she could continue to go online with confidence to pay bills, read the online edition of her hometown newspaper, and purchase her favorite perfume and other hard-to-find items. Also, instead of keeping her story

to herself, she decided to get even with the cyberthieves who tricked her. "My way of getting even," Melloon said, "is to help spread the word about online safety, and help prevent the crooks who robbed me from robbing other people."

She found a pulpit for her message through a cybersafety campaign organized by AARP Washington and co-sponsored by Microsoft, the Washington state attorney general's office and the Federal Trade Commission. The campaign is one of the latest examples of the AARP and Microsoft working together to spread the word about online safety.

Not limited just to seniors, the cybersafety campaign instructed attendees about how to recognize and avoid cyberscams and other online maladies, such as viruses and phishing e-mails. Attendance at the events exceeded expectations in every community, filling conference rooms at every stop — in big cities, rural communities and bustling suburbs. In two locations second sessions were added, demonstrating that consumers truly want and

need more information about how to stay safer online.

"The turnout was stunning," said Kristin Johnsen, senior director of security outreach for the Security Technology Unit at Microsoft, who presented information about security technologies and services at several stops on the tour. Following each event Johnsen was swarmed by people with questions. "People are looking for answers, and are thrilled to get expert help on how to take more control of their Internet experience," she said.

Art Cruz, state president for AARP Washington, spoke to the tour attendees who were reluctant to shop, pay bills or do other tasks online out of concern about identity theft. "This campaign has given them the knowledge they need to help protect their computers, and the confidence to take advantage of many more of the things you can do online," Cruz said.

In addition to expert advisors, the campaign featured older computer users who had been victims of cybercrime.

Melloon overcame her fear of public speaking to recount her story to more than 300 people at one event. She also appeared in an AARP informational DVD, which has been distributed to thousands of people statewide. In her community, she has done television interviews and appeared in her hometown newspaper advocating online safety.

Melloon, who works as a blackjack dealer at a casino near her home, said she has learned not to gamble when it comes to her online safety. She no longer opens e-mail from senders she doesn't know, and checks to ensure the authenticity of e-mail messages and Web sites before entering any personal information. She's also updating her security software, anti-virus and anti-spyware protection.

"I'm an ordinary person who uses the computer to do ordinary things, but I got caught," she said. "You really have to think before you click."

the first line of online defense

What: A firewall is software that helps prevent hackers, viruses and worms from accessing your computer over the Internet. Firewalls do not detect or disable computer viruses and worms if they are already on your computer. For that reason, you should also install anti-virus and anti-spyware software and keep them updated to help prevent viruses, worms and other security threats. If you have Microsoft Windows XP Service Pack 2 running on your computer, you can check to see if your firewall is turned on through the Windows Security Center. To get to the Windows Security Center, click on Start, the Control Panel, Security Center, Windows Firewall.

Why: Hackers can gain access to personal information or install code that destroys files or causes malfunctions, or they can turn your computer into a "zombie." This happens when a hacker takes over your computer and uses it to attack other computers.

How: The firewall within Windows monitors all incoming and outgoing information within your Internet connection, and helps prevent unsolicited incoming "traffic" from reaching your computer.



Firewalls temporarily open doors, or "ports," on your computer to receive traffic that you have requested, such as a Web page.

Where: Windows XP SP2 includes a built-in firewall, which is turned on by default. When it is released, Windows Vista will include a built-in firewall that will help protect you from both incoming and outgoing viruses and worms. Windows Live OneCare also provides two-way firewall functionality to help keep the bad stuff out and the good stuff in. That outbound protection can help prevent malware or malicious programs from sending information out from your computer without you knowing. For information about firewalls for other operating systems and from other software companies (including free trials), visit <http://www.microsoft.com/protect>.

how to spot an online scam

Some people can sniff out a scam from a mile away. Some can't, or their scam detectors are thrown off when crooks use a new tactic or technology. One of the newest and most rampant scams, called "phishing," is helping fuel identity theft nationwide. These cybercriminals try to lure people in with what look to be legitimate e-mail requests from trusted companies. Here are some do's and don'ts for avoiding "phishing" and other online scams:

Do:

- Type Web addresses listed in e-mail messages into your browser or use your personal bookmarks. Don't click on links within e-mail, especially if you don't know the sender. Even if the message displays the correct Web address, links in some fraudulent messages may take you directly to phony sites where you could unknowingly transmit personal or financial information.
- Update your computer software. The Automatic Updates feature within Windows provides security updates that help protect you from many malware and online scams that are delivered via e-mail. Learn more here: <http://www.microsoft.com/protect>.
- Make sure a Web site is secure before you enter personal or financial information. In Internet Explorer, check for a yellow lock icon on the status bar as shown below. In other services, you may see an unbroken key. To help increase your safety, double-click on the icon to display the security certificate for the site. The name following "Issued to" should match the name of the site.
- Take advantage of anti-phishing software to help protect you from scam e-mail and Web sites. Microsoft offers free protection tools with Microsoft SmartScreen Technology for e-mail and Microsoft Phishing Filter to help protect you when you're browsing. Other companies also offer anti-phishing protection tools too.

Don't:

- Don't follow enticing online offers if you are asked to provide money up front, pay a processing fee or cover the cost of expediting the sale.
- Don't trust photocopied documents. Photocopies of government certificates, banking information or other documents should not be trusted as evidence that a sender's offer is legitimate; such documents are almost always fake.
- Don't enter personal or financial information into pop-up windows. Some scam artists create fake pop-up windows that open when you click on a link in legitimate-looking e-mail messages.
- Don't keep quiet. If your personal information has been compromised, immediately report the circumstances to the following authorities:

Your local police. A police report will help establish with your bank, credit card company and other institutions that you are the victim of a crime and not a credit abuser.

Your credit card company and/or bank, if you have given out your credit card or bank account information.

The company whose Web site was forged. Contact the company directly, not through the fraudulent e-mail message.

The Federal Trade Commission. Contact the FTC's National Resource About Identity Theft Web site (<http://www.consumer.gov/idtheft>) to learn how to minimize the damage from identity theft.

don't get trapped in your own web social circle

The next time somebody asks you how big your social circle is, tell them it stretches around the world — from Tokyo to Timbuktu. You won't be lying if you are one of the millions of teens who maintain a blog or other online networking site. In fact, a Georgetown University study found that half of all blog sites are owned by teenagers.

With personal networking sites, you can keep your friends up to date about how school's going, what your favorite recent MP3s are, or what happened on your vacation. You can also see what other people are doing on their sites, and learn lots of cool things about the people you meet online. But in the midst of doing all those interesting things, you've probably also come across some strange people. And when interacting online, sometimes we make ourselves a target for these types of people without knowing it — even when we think we're being careful.

Fourteen-year-old Susan is a perfect example. Like many teens, she spends a lot of time online and has accumulated a good collection of "friends" on her personal site. She's smart and conscientious, and thinks she's playing it safe. **Safety & Security Online** asked Kristin Johnsen, senior director of security outreach for the Security Technology Unit at Microsoft, and Staca Urie, manager of outreach for the NetSmartz Workshop at the National Center for Missing & Exploited Children, to review some comments from Susan about her online habits. As you'll see, Susan is putting herself at risk of getting tangled in her own online social Web, without even knowing it.

SUSAN: I do put my first and last name (on my site). I don't write blogs, but I have friends who do — what they put up is what they did today or how they feel at the time, but it's not, in my opinion, something anyone would look at and get the wrong impression. In my opinion, if you read someone's blog, then you kind of know that person and, if not, what are you going to do besides read something about someone that you don't know?

The mistake there, according to Johnsen, is that bad guys won't pass by a personal site just because they don't know the person who owns it. "Predators gather information over time, not just from one read," Johnsen said. "They put together pieces of information that dribble out, in photos or the places referenced in your postings." Even listing the concerts you see can help a predator figure out where you live. They will look for hints about when your parents are at work or other times when you might be home alone. "If you post too much information, like your picture or even your full name," said Johnsen, "you are doing the predator's homework for them." For example, if you post a picture of you in front of your school or wearing your letter jacket, you can provide clues about your location, Johnsen said.



SUSAN: I say that I'm 16 on one (personal) site and 14 on the other. You have to be over 16 to have an account on this service, but it says on my profile that I was born in '91, so it's not like I'm trying to be 16, it's just that you have to be over a certain age and until I am that age, I have to be the lowest age possible ... I have friends in sixth and seventh grade who have a blog or Space.

Lying about your age can lead to problems because it exposes you to potential risks you're not prepared to deal with and may not foresee, said Urie. You may enjoy the attention you get from online friends, but predators know this and may exploit that fact to establish a relationship with you. For example, they may try to draw you in by offering you items from your "wish list" or registry of things you want. "One of the first rules we learn as kids is not to accept gifts from someone you just met," said Urie. "The rule is doubly true online."

"Windows Live Spaces offers users the ability to manage their own settings so they are in control of who is in their social network and who views their Windows Live Spaces site," said Johnsen. "Those users whose profile indicates they are under 18 are automatically defaulted to a more restrictive setting for others to view their Space: only those on their Windows Live Messenger contact list may do so. In addition, for the 'friends of friends' social networking feature, this restrictive default setting is used for all customers. These measures help Windows Live Spaces users avoid unwanted contacts or contacts from persons they don't know or don't have a trusted connection with — like a mutual friend."

SUSAN: My parents have told me the risks, and I know what the situation is... I don't think they quite understand the situation half the time. I know there are cases where someone has gotten hurt over the Internet. But I'm smart enough ... as long as you know the risks, I feel that's kind of all you can do at the moment.

The best way to protect yourself — and ease your parents' fears — is to communicate openly about what you are doing online, according to Urie. You might worry that your parents will restrict your Internet access if you share information about a scary or uncomfortable situation, but you need to speak up, said Urie: "If you feel threatened, your parents will be your best protection."

It's best to take action before problems arise. Here's a reminder of some key tips to remember:

- **Keep your personal information personal.** Avoid posting anything that might identify you. That includes your full

name, the name of your school, sports teams, the town you live in or where you hang out, and more.

- **Protect your information.** Check to see if your service allows you to control who can visit your profile or blog. If so, allow only people you know and trust; if not, find another service.
- **Avoid in-person meetings.** Don't get together with someone you "meet" in a profile or blog or while IMing unless you are certain of their actual identity and get your parents' approval. Although it's still not risk-free, if you do meet the person, arrange the meeting in a public place and bring some friends along.
- **Photos: think before posting.** What's uploaded to the Net can be downloaded by anyone, passed around, changed and posted online forever. So remember the "embarrassment rule": Don't post anything you wouldn't want seen by a parent or grandparent, college admissions counselor, or future employer.
- **Check comments regularly.** If you allow them on your profile or blog, check them often. If there are mean or embarrassing comments, don't respond. Delete them and, if possible, block those people from commenting further.
- **Be honest about your age.** Membership rules are there to help protect people. If you are too young to sign up, talk with your parents about alternative sites that may be appropriate for you.

And remember, not everyone is who they say they are on the Net. Chatting and postings can be seen by lots of people around the world, including those who you might not want to. If you experience problems through your blog and feel you are in danger, tell an adult and the police. If you feel personally threatened, you can also report the incident to your site service, to one of the online resources below, and your parents or an adult.

To make a report, contact the CyberTipline at <http://www.cybertipline.com>. For additional information, visit the following sites:

- i-SAFE Inc.: <http://www.isafe.org>
- NetSmartz: <http://www.netsmartz.org>
- OnGuard Online: <http://onguardonline.gov>
- SafeKids.com: <http://www.safekids.com>
- StaySafe.org: <http://www.staysafe.org>

You can find the rest of the interview with Susan and her mother at StaySafe.org.

put your online smarts where your mouth is

share what you know with others

Sure, you can track down a new band's Web site in less than a minute, and the comments section on your blog is beginning to look like the last novel you had to read for English class. But do you know how to stop online criminals from hijacking your computer? And do you know what to do if someone you don't know starts IMing you constantly?

If not, you can continue building your repository of cyberskills by learning more about Internet safety and getting active in efforts to spread the word. i-SAFE, an online safety organization, offers a variety of programs to help teens learn more about online safety and share their newfound knowledge with their friends, their siblings, and even their teachers and parents. Programs include these:

- **i-DRiVE TV** lets you create video reports and interviews and contribute them to an i-SAFE "news" broadcast. Get the 411: <http://xblock.isafe.org/idrive.php>.
- **i-MENTOR** will help you learn how to share what you know about technology and online safety with your friends and other students. Get the 411: <http://www.ilearn.isafe.org>

survey

teen bloggers freely share personal information online

How much personal information do you share online? If you're worried that you share too much, you're not alone. A recent Northwestern University study found that a significant percentage of teens willingly share more information than online security experts say is safe. To help avoid cyberstalkers and cyberbullies, online security experts say teens should not share anything other than their first name on blogs, social networking sites or in e-mail with people they don't know in person. Here's the kind of information that teen bloggers said they share:

70%

disclosed at least their first names

67%

provided a feedback section on their blogs

61%

provided their contact information

44%

provided their instant messenger name

30%

provided a link to their home page

50%

provided a link to other bloggers

50%

included discussions about peers

66%

disclosed at least their first name AND age

59%

disclosed their city or state

Source: David Huffaker, "Teen Blogs Exposed: The Private Lives of Teens Made Public," a study of 68 randomly selected weblogs produced by teenagers age 13 to 17, 2006



Keeping people safe online is a big job — too big, in fact, for any one company, organization or government agency. Once set free, viruses and spyware can rapidly spread to millions of computers worldwide, requiring software companies and law enforcement agencies to pool their knowledge and resources to stop Internet threats. As the range of online activities has grown, so has the range of people who take advantage of the Internet. Each of these groups — from youngsters to seniors — has different interests and technology skills. As a result, each requires different types of educational materials and resources to help people stay safe online.

To overcome these challenges, a broad range of previously unaffiliated companies, organizations and government agencies have begun working together to make the Internet a safer place to learn, play and do business. In some cases, even competitors are working together to help their mutual customers. Safety & Security Online gathered perspectives from a variety of organizations that have teamed up with Microsoft and other groups in recent years to increase safety and security online:

- **Jonathan King**, director of professional development and outreach at i-SAFE, a nonprofit foundation dedicated to protecting the online experiences of young people through classroom curriculum and community outreach.
- **Staca Urie**, manager of outreach for the NetSmartz Workshop, a NCMEC program dedicated to preventing the online victimization of children.
- **Kristin Johnsen**, senior director of security outreach for the Security Technology Unit at Microsoft.



working together

Q: Why is it important for organizations such as yours and companies like Microsoft to work together to improve the online security practices of consumers?

King: i-SAFE looks at the Internet as an online community with rules and codes of conduct, just like any other community. Everybody on the Internet needs to be taught how to be a good cybercitizen — and how to protect themselves from people who refuse to play by the rules. We don't expect any one group or organization to educate people how to be good citizens in the offline world; we do it collectively. We must do the same for cybercitizenship.

Urie: By working together, we can speak with one voice. Consistent messages and guidance have more impact, and the broader the group of partners, the broader the audience we can attract. Together, we can expose many more people to more information and resources than they might see if they connected with just one of the partner organizations.

Johnsen: More than 80 percent of Americans online have not taken appropriate computer protection measures and are at risk for online criminal activity or virus and spyware problems. We at Microsoft are determined to help make the Internet safer for everyone, especially children and families. But we can't do it alone. The organizations we work with are experienced leaders known for educating their audiences. They are committed to helping people get and stay safe online, and are working with Microsoft to help raise public awareness of online safety issues and best practices for staying protected.

to increase online safety and security

vocabulary lesson

SPYWARE
PRONOUNCED \SPY-WARE\

n. Any software that covertly gathers information about a user while he/she navigates the Internet and transmits the information to an individual or company that uses it for marketing or other purposes.

Q: How do your collective efforts to educate people about online safety differ from those you can offer individually?

Johnsen: The Get Net Safe tour is a great example of what we can offer people when we work together. We have combined the resources of 11 organizations to reach a broader cross-section of people than any other education effort I've worked on. Together we have put on assemblies at elementary, middle and high schools, and hosted school parents' nights to spread our message to other family members. Boys & Girls Clubs have staged Internet safety fairs. Local chambers of commerce have held cybersecurity forums for community leaders and small-business owners.

Q: What results have your collaborations with Microsoft produced?

Urie: Recently, NCMEC worked with Microsoft to distribute AMBER Alerts via MSN Mobile, MSN Hotmail, Windows Live Mail, MSN Messenger and Windows Live Messenger. The millions of people in the United States who use MSN and beta Windows Live services receive timely bulletins of the most serious child abduction cases in their communities. This is a powerful use of technology that will allow us to get information about missing children to more people who can be on the lookout.

King: We worked with Microsoft to make our professional education program available online. Educators and parents can earn i-SAFE certification by completing a course that we offer online. With Microsoft's support, we've been able to expand this effort by adding the i-MENTOR Training Network for students, in which students teach their peers and younger children about how they can help stay safe online. We also recently expanded our offering with i-PARENT and i-FIFTY+ to help teach parents and seniors be more safe while using the Internet. Microsoft provided

the resources to develop those training programs, enabling us to offer more substantive online safety education.

Q: What else are your organizations doing to promote online safety?

Johnsen: Microsoft supports law enforcement by providing them with technical training, investigative and forensic assistance, and the development of new technology tools to combat cybercrime. In addition, our collaborations with law enforcement have helped crack down on online criminals. Earlier this year, we provided Bulgarian law enforcement with information that helped them arrest eight people suspected in an international criminal network involved in financial fraud and stealing personal data via the Internet. Also, one of the world's most prolific spammers — a guy who called himself "Spam King" — agreed to fundamentally change his practices and forfeited millions of dollars of his ill-gotten gains after Microsoft and the New York attorney general jointly sued him.

King: At i-SAFE, we want to bring Internet safety education to every student in the United States. But we're also working with Microsoft on an international initiative, creating packages and solutions to provide to other countries. These provide localized information applicable to the area in which the package will be used, allowing people to take it and grow the messages from within. Our goal is to provide the resources and nurture people in these areas so that when they do come online, they can be safe and responsible.

Urie: Recently NetSmartz partnered with the Internet Crimes Against Children Task Forces to provide law enforcement with interactive assemblies for parents, students and community members. NetSmartz provides law enforcement teams with the material they need to deliver Internet safety messages. In addition, we post new material frequently on our Web site. Recently we added information on social networking sites, cyberbullying and how to "use your NetSmartz" (UYN).

resources expand online education options

In search of online safety and security information and resources?
Check out these helpful Web sites:

AARP delivers a collection of online resources, technology reviews and guides geared to the interests of seniors: <http://www.aarp.org/learntech/computers> and <http://www.aarp.org/netsafe>.

American Academy of Pediatrics offers guidelines for regulating children's use of the Internet and other media: <http://www.aap.org/healthtopics/mediause.cfm>.

GetNetWise is a user empowerment campaign and Web site designed to offer Internet users a user-friendly, easy-to-find, online resource that can be found on the most popular entry points to the Internet as well as on many of the most popular Web sites: <http://www.getnetwise.org>.

i-SAFE offers training and curriculum resources for educators, and training for teens, parents and 50+ to become community mentors. Online training can be found at www.ilearn.isafe.org.

National Center for Missing & Exploited Children offers information about how to report missing children and tips on how to protect children online: <http://www.missingkids.com>.

National Cyber Security Alliance provides tools and resources to empower home users; small businesses; and schools, colleges and universities to stay safe online: <http://www.staysafeonline.info>.

NetSmartz.org is an interactive, educational safety resource created by the National Center for Missing & Exploited Children to teach kids and teens how to stay safer on the Internet: <http://www.netsmartz.org>.

Onguard Online provides people with practical tips from the federal government and the technology industry to help them be on guard against Internet fraud, secure their computers and protect their personal information: <http://www.onguardonline.gov>.

StaySafe.org is an educational site intended to help consumers understand both the positive aspects of the Internet and how to manage a variety of safety and security issues that exist online: <http://www.staysafe.org>.



online safety information cards



protect your PC quick tips for safer internet use

- **Use an Internet firewall.** Firewall software serves as a first line of online defense by helping block malicious hackers, viruses and worms before they reach your computer.
- **Keep current.** With the Automatic Updates feature enabled, Windows® Update can deliver high-priority security updates to your computer as they become available. You can decide when and how security updates are installed.
- **Install anti-virus protection.** Managed anti-virus programs that are always on and keep themselves up to date, such as the one included in Windows Live™ OneCare™, help protect you from malicious programs called viruses that can slow down your PC or destroy files, as well as attach themselves to a program or file to spread from computer to computer. Also keep an eye on your subscription to help ensure your anti-virus program subscription doesn't expire, creating a lapse in your protection.
- **Install anti-spyware software.** Anti-spyware software, such as the Windows Defender beta, helps protect your computer from programs that can track your Web-browsing habits or make changes to your computer settings without your consent or control. See if you already have it by clicking on Start and then All Programs. From there, look for the words "spy," "Spyware" or "anti-spyware." For more information on why anti-spyware software is important and how to get it, visit <http://www.microsoft.com/protect>.



online safety information cards

downloads, other resources to help protect your PC

Internet firewall frequently asked questions:
<http://www.microsoft.com/protect>.

Microsoft Update helps keep your security and other software current: <http://update.microsoft.com>.

Windows Defender helps protect against spyware:
<http://www.microsoft.com/protect>.

Windows Live OneCare includes anti-virus, anti-spyware, firewall, performance tuneups, and file backup and restore functionality. For a free trial, visit <http://onecare.live.com>.

Windows Live OneCare Safety Scanner is a free, on-demand online resource that helps consumers protect themselves and their families online and keep their PCs healthy and running well: <http://safety.live.com>.

Additional security software downloads and several free trials from various companies are available at <http://www.microsoft.com/protect>.



online safety information cards



protect yourself quick tips for safer internet use

- To help avoid computer viruses that spread through e-mail and to help avoid receiving additional unwanted e-mail, delete spam and use care in opening unexpected attachments. Also, enable the anti-spam features that may be offered with your e-mail.
- Review a Web site's privacy policy before sharing personal information on it. The privacy statement should tell you how and why a business is collecting your personal information and how it plans to use it. If something doesn't sound right to you, contact the company with questions before you share any personal information. If the site does not post a privacy policy, take your business elsewhere.
- Before entering your credit card or other personal information on a Web site, make sure the Web address begins with https — the "s" stands for "secure" — (for example, <https://www.tailspintoys.com>) and look for an icon of a tiny locked, golden or glowing padlock. 
- Create strong passwords to help protect your identity. Passwords should contain eight or more characters and include a combination of numbers and symbols, along with uppercase and lowercase letters. For instance, replace a letter with a common symbol, such as a "\$" for an "S."
- Use services, such as the Microsoft® Phishing Filter, that provide alerts when you visit suspected sites which might try to trick you into divulging personal information. Microsoft Phishing Filter is available in the Live Toolbar and will be included in Windows® Internet Explorer® 7 for Windows XP and Windows Vista.



help protect your family quick tips and reminders

- **Protect identities.** Kids should use a gender-neutral screen name, and never divulge online their real name, address, age or other information that can be used by criminals to locate them, including school, sports team or friends' or family members' names or other personal information.
- **PC proximity.** Consider placing the family computer in a common room, where supervision and use guidelines are easier to enforce.
- **Filter content.** Restrict access to Web sites and content individualized for each member of the family with services such as the Windows Vista™ Family Safety Parental Controls and Windows Live™ OneCare™ Family Safety.
- **Create a contract.** Keep communication open between parents and children and learn about the family's activities on the Web. Then, develop an Internet "code of conduct and usage agreement" with house rules based on a child's age, and have all family members sign the contract.



online safety information cards

help protect yourself online

Test your passwords. The following site offers an automated service that measures the relative safety of your passwords against Microsoft’s recommended precautions: <http://www.microsoft.com/protect>.

Windows XP Protection Features:

These sites teach you to do the following:

- **Set permissions for shared files and folders.** Learn how to restrict access to your files: <http://www.microsoft.com/windowsxp/using/security/learnmore/tips/stevens1.msp>.
- **Encrypt your data.** Learn how to convert files and folders into a format that can’t be read by other people: <http://www.microsoft.com/windowsxp/using/security/learnmore/encryptdata.msp>.
- **Lock your computer.** Learn how to quickly restrict access to your computer without logging off: <http://www.microsoft.com/windowsxp/using/security/learnmore/tips/schnoll1.msp>.
- **Use backup capabilities to help protect your data.** Learn how to create an extra copy of important files in case your computer fails or is lost or stolen: <http://www.microsoft.com/windowsxp/using/security/learnmore/backup.msp>.

downloads, other resources to help protect your family online

Ask an expert. Pose questions about online safety at http://www.staysafe.org/q_and_a/2006-05.html

CyberTipline. This NCMEC Web site enables visitors to receive guidance about and report child exploitation: www.cybertipline.com

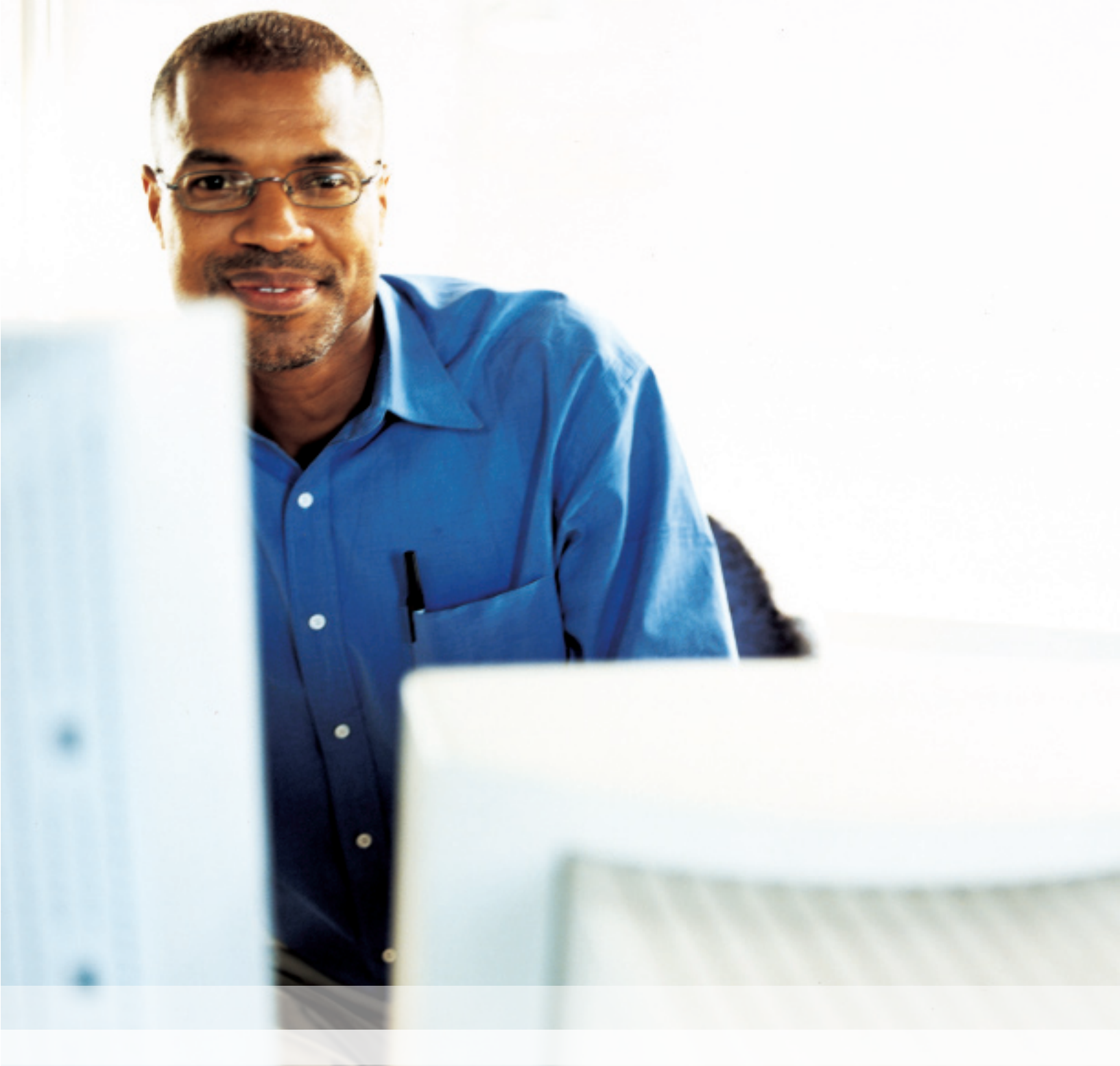
Get doctors’ advice. Guidelines from the American Academy of Pediatrics on how to regulate children’s use of the Internet and other media can be found at <http://www.aap.org/healthtopics/mediause.cfm>.

i-SAFE i-PARENT Times. This monthly online publication features up-to-date online safety guidance for parents: <http://www.isafe.org/newsletter/iparent.html>

Kid-safe sites. Expert-approved sites with content appropriate for children are listed at <http://kids.getnetwise.org/kidsites>.

Law enforcement contact information. Report online crimes against children at <http://kids.getnetwise.org/trouble/#contact>

Windows Live OneCare Family Safety. This free service is currently in beta; when it is formally launched it will include content filtering for the Web, contact list management tools for communication services, and online activity reports. More information can be found at <http://ideas.live.com>.



I hunt worms for a living

Microsoft has a team of attorneys and investigators who provide investigative support to help track down computer hackers. Microsoft helped law enforcement authorities in Turkey and Morocco arrest the alleged authors of the Zotob and Mytob worms — within two weeks after the worms were

unleashed. Microsoft worked closely with the FBI and law enforcement overseas in the investigation. In 2004, Microsoft awarded \$250,000 to two individuals who helped identify the creator of the notorious Sasser worm. The author of the worm was recently found guilty by a court in Germany.



microsoft.com/protect

© 2006 Microsoft Corp. All rights reserved.

Microsoft, Hotmail, Internet Explorer, MSN, OneCare, SmartScreen, Windows, Windows Live, Windows Server, Windows Vista, Xbox, Xbox 360 and Xbox Live are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries.

Bluetooth is a trademark owned by the Bluetooth SIG Inc. and any use of such marks by Microsoft Corp. is under license.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.